



日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出 願 年 月 日

Date of Application:

2000年12月20日

出 願 番 号

Application Number:

特願2000-387833

[ST.10/C]:

[JP2000-387833]

出 願 人

Applicant(s):

株式会社セガ

RECEIVED

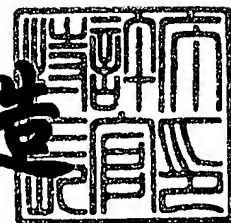
FEB 06 2002

Technology Center 2600

2002年 1月11日

特許庁長官  
Commissioner,  
Japan Patent Office

及川耕造



出証番号 出証特2001-3115017

【書類名】 特許願

【整理番号】 S007P3P111

【あて先】 特許庁長官殿

【発明者】

    【住所又は居所】 東京都大田区羽田1丁目2番12号  
                        株式会社ソニックチーム内

    【氏名】 見吉 隆夫

【発明者】

    【住所又は居所】 東京都大田区羽田1丁目2番12号  
                        株式会社ソニックチーム内

    【氏名】 節政 暁生

【特許出願人】

    【識別番号】 000132471

    【氏名又は名称】 株式会社セガ

【代理人】

    【識別番号】 100079108

    【弁理士】

    【氏名又は名称】 稲葉 良幸

【選任した代理人】

    【識別番号】 100080953

    【弁理士】

    【氏名又は名称】 田中 克郎

【選任した代理人】

    【識別番号】 100093861

    【弁理士】

    【氏名又は名称】 大賀 眞司

【手数料の表示】

    【予納台帳番号】 011903

    【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9706518

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 セキュリティシステム

【特許請求の範囲】

【請求項 1】 通信ネットワークに接続するデータ処理装置に固有の識別情報を発行する手段と、該データ処理装置に固有の識別情報と該データ処理装置にて処理されるべきデータを記録した記録媒体に固有の識別情報とを関連付けて記憶する手段と、該関連付けを参照することで何れの記録媒体が何れのデータ処理装置で使用されたかを管理する手段と、を備えたセキュリティシステム。

【請求項 2】 前記データ処理装置に固有の識別情報として、データ処理装置が通信ネットワークに接続した時期又はこれを利用した情報を用いる請求項 1 に記載のセキュリティシステム。

【請求項 3】 通信ネットワークに接続するデータ処理装置に固有の識別情報を発行し、該データ処理装置に固有の識別情報と該データ処理装置にて処理されるべきデータを記録した記録媒体に固有の識別情報とを関連付けて記憶し、該関連付けを参照することで何れの記録媒体が何れのデータ処理装置で使用されたかを管理する記録媒体管理方法。

【請求項 4】 前記データ処理装置に固有の識別情報として、データ処理装置が通信ネットワークに接続した時期又はこれを利用したを用いる請求項 3 に記載の記録媒体管理方法。

【請求項 5】 請求項 3 又は請求項 4 に記載の記録媒体管理方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 6】 通信ネットワークを介してサーバから発行されるデータ処理装置に固有の第 1 識別情報を記憶する記憶手段と、データを記録した記録媒体に固有の識別情報であって上記第 1 識別情報とともに関連付けられて記録媒体の管理に用いられる第 2 識別情報を第 1 識別情報とともに通信ネットワークを介してサーバに送信する送信手段と、を備えたデータ処理装置。

【請求項 7】 コンピュータシステムを請求項 6 に記載の記憶手段、及び送信手段として機能させるプログラムを記録したコンピュータ読み取り可能な記録

媒体。

【請求項 8】 バックアップメモリのセーブデータをデータ処理するデータ処理装置であって、セーブデータを該データ処理装置に固有の識別情報をキーとして暗号化処理する手段を備えたデータ処理装置。

【請求項 9】 前記暗号化処理されたセーブデータを前記識別情報をキーとして復号化処理する手段を備えた請求項 8 に記載のデータ処理装置。

【請求項 10】 バックアップメモリのセーブデータをデータ処理装置に固有の識別情報をキーとして暗号化処理するデータ処理方法。

【請求項 11】 前記暗号化処理されたセーブデータを前記識別情報をキーとして復号化処理する請求項 10 に記載のデータ処理方法。

【請求項 12】 請求項 10 又は請求項 11 に記載のデータ処理方法をデータ処理装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 13】 バックアップメモリに記憶されているセーブデータを読み取って記憶する手段と、該セーブデータの読み取り終了後にバックアップメモリに記憶されているセーブデータを消去する手段と、を備えたデータ処理装置。

【請求項 14】 データ処理装置にてデータ処理されるセーブデータをデータ処理装置に転送した後で、バックアップメモリ内の不揮発性メモリに記憶されたセーブデータを消去するセーブデータの管理方法。

【請求項 15】 バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した回数をデータベースに登録するとともに、上記回数をバックアップメモリ又はデータ処理装置に記録する手段と、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した際にデータ処理装置から取得した上記回数がデータベースに登録されている回数と一致した場合にバックアップメモリ内のデータの処理を許可する手段とを備えたセキュリティシステム。

【請求項 16】 前記バックアップメモリに固有の識別情報として、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した時期又はこれを利用した情報を用いる請求項 15 に記載のセキュリティシステム。

【請求項 17】 バックアップメモリを備えたデータ処理装置が通信ネット

ワークに接続した回数をデータベースに登録するとともに、上記回数をバックアップメモリ又はデータ処理装置に記録し、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した際にデータ処理装置から取得した上記回数がデータベースに登録されている回数と一致した場合にバックアップメモリ内のデータの処理を許可するセーブデータの管理方法。

【請求項 1 8】 前記バックアップメモリに固有の識別情報として、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した時期又はこれを利用した情報を用いる請求項 1 7 に記載のバックアップメモリ管理方法。

【請求項 1 9】 請求項 1 7 又は請求項 1 8 に記載のバックアップメモリ管理方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 2 0】 ゲームの難易度に対応して通信ゲームに参加可能なレベルを予め設定し、ゲームの難易度に対応した要求レベルを満たすプレイヤーに対して通信ゲームの参加を許可するゲームサーバ。

【請求項 2 1】 通信ネットワークに接続して通信ゲームを行うときにはゲームの進行状況をセーブデータとして保存しないゲーム処理方法。

【請求項 2 2】 請求項 2 1 に記載のゲーム処理方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 2 3】 通信ネットワークに接続して通信ゲームを行うときにはゲームのエンディング画面の表示時間を短くするゲーム処理方法。

【請求項 2 4】 請求項 2 3 に記載のゲーム処理方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は複数のゲーム装置がネットワークに接続して行う通信ゲームの改良技術に関する。

【0 0 0 2】

【従来の技術】

複数のゲーム装置が電話回線、ISDN網等の通信ネットワークに接続し、通信ゲームを行うことが提案されている。かかる通信ゲームにおいて、本出願人はゲームソフトウェアを記録した記録媒体の第三者による不正使用を防止するべく、特開平2000-35885号にて記録媒体のセキュリティ技術を提案した。

【0003】

同公報に記載の技術はゲームソフトウェアを記録した記録媒体に固有の識別情報とゲーム装置に固有の識別情報をサーバが一元管理し、どのゲーム装置がどの記録媒体を使用したかを把握しておくことで、ゲーム装置が通信ネットワークに接続したときに、そのゲーム装置に装着された記録媒体が以前に他のゲーム装置に使用されたものであるとサーバが判断したときにはゲーム処理に制限を設け、当該ゲーム装置にのみ使用されたものであるとサーバが判断したときには通常のゲーム処理を行うというものである。

【0004】

【発明が解決しようとする課題】

しかし、ゲーム装置に固有の識別情報は必ずしもゲーム装置の開発の段階で予め入れておくとは限らないため、このような識別情報を持たないゲーム装置も存在する。

【0005】

また、通信ゲームにおいては、ゲーム装置本体或いは操作用コントローラに脱着可能に構成されたバックアップメモリにゲームの進行状況やプレイヤーが獲得した各種アイテム等のデータを待避保存しておくことで、ゲーム終了直前の状態から再びゲームプレイを行うことができていたが、バックアップメモリの内容をコピーすることで、第三者に自己のセーブデータ（例えば、アイテム等）を提供することができるため、当該第三者は他人のセーブデータを利用してゲームを楽しむことができた。このようにバックアップメモリの内容が容易にコピーされると、プレイヤーがゲームの面白さを味わうことができないという不具合が生じる。

【0006】

このような問題はゲーム装置本体或いは操作用コントローラに脱着可能に構成されたバックアップメモリを他人のゲーム装置本体或いは操作用コントローラに



装着してゲームプレイを行うことができるように構成した場合にも生じる。

【0007】

また、バックアップメモリに待避保存されたセーブデータを通信ネットワークを介してゲーム装置から他のゲーム装置に転送することができるが、バックアップメモリからゲーム装置にセーブデータを転送する際にバックアップメモリ内にセーブデータを残しておく、バックアップメモリをゲーム装置から強制的に抜き取ることで自己のバックアップメモリにセーブデータを残したまま、他人にセーブデータを提供することができるという不正使用がなされるおそれがある。

【0008】

また、従来の通信ゲームにおいてはゲームに参加可能なレベルに制限を設けなかったため、例えば、初心者と上級者が通信ゲームに参加する場合には、初心者は何もしなくても上級者の後をつけて行くことでゲームのエンディングにまで辿り着いてしまうことになり、ゲームの面白さが半減する結果となっていた。

【0009】

同様に、複数の遊戯者が参加する通信ゲームの場合にゲームの進行状況に関するセーブデータを待避保存しておく、初心者は上級者とともにゲームに参加することで上級者のゲームの途中からゲームを進めることとなってしまう。初心者のバックアップメモリにゲームの進行状況に関するセーブデータを保存してしまうと、次回のゲームはこの途中から開始することとなってしまう、ゲームの一部がプレイできなくなってしまうまになるため望ましくない。

【0010】

また、通信ゲームの場合は電話回線に接続している限り、接続料として電話料金が課金され、さらにプロバイダへのインターネット接続料も課金されるため、遊戯者の操作を必要としないゲームのエンディングが必要以上に長時間を要すると、プレイヤはゲームプレイをしていないのにもかかわらず、過大な経済的負担を強いられる結果となる。

【0011】

そこで本発明は、第三者による記録媒体の不正使用を防止するセキュリティシステム、データ処理装置、記録媒体管理方法及び該方法を実行するためのプログ

ラムを記録したコンピュータ読み取り可能な記録媒体を提案することを課題とする。また本発明はバックアップメモリの不正使用を防止するデータ処理装置、データ処理方法、セキュリティシステム、セーブデータの管理方法及び該方法を実行するためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提案することを課題とする。また本発明は通信ゲームをより面白く楽しむためのゲームサーバ、ゲーム処理方法及び該方法を実行するためのプログラムを記録したコンピュータ読み取り可能な記録媒体を提案することを課題とする。

## 【 0 0 1 2 】

## 【課題を解決するための手段】

上記の課題を解決するべく、本発明では通信ネットワークに接続するデータ処理装置に固有の識別情報を発行し、該データ処理装置に固有の識別情報と該データ処理装置にて処理されるべきデータを記録した記録媒体に固有の識別情報とを関連付けて記憶し、該関連付けを参照することで何れの記録媒体が何れのデータ処理装置で使用されたかを管理する。データ処理装置の識別情報は通信ネットワークを介してサーバが発行するため、予め固有の識別情報を持たないデータ処理装置であっても、記録媒体のセキュリティを確保することができる。

## 【 0 0 1 3 】

また本発明では上記の方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体を提供することができる。コンピュータ読み取り可能な記録媒体として、例えば、光ディスク（CD-ROM、DVD-ROM、DVD-RAM、DVD-R、PDディスク、MDディスク、MOディスク等の固有の物理フォーマットをもつディスク）やフレキシブルディスク（FD）のように可搬性記録媒体の他、RAMやROM等のコンピュータ内の内部記憶装置、或いはハードディスクのような外部記憶装置等がある。

## 【 0 0 1 4 】

また本発明ではバックアップメモリのセーブデータをデータ処理装置に固有の識別情報をキーとして暗号化処理する。これにより、バックアップメモリ内のセーブデータは他のデータ処理装置では使用できないため、セーブデータの不正使用を防止することができる。

## 【0015】

また本発明ではデータ処理装置にてデータ処理されるセーブデータをデータ処理装置に転送した後で、バックアップメモリ内の不揮発性メモリに記憶されたセーブデータを消去する。これにより、バックアップメモリ内のセーブデータを該バックアップメモリ内に残したまま他のデータ処理装置に転送するという不正使用を有効に防止することができる。

## 【0016】

また本発明ではバックアップメモリを備えたデータ処理装置が通信ネットワークに接続した回数をデータベースに登録するとともに、上記回数をバックアップメモリ又はデータ処理装置に記録し、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した際にデータ処理装置から取得した上記回数がデータベースに登録されている回数と一致した場合にバックアップメモリ内のデータの処理を許可する。これにより、バックアップメモリ内のセーブデータの不正コピーを有効に防止することができる。

## 【0017】

また本発明ではゲームの難易度に対応して通信ゲームに参加可能なレベルを予め設定し、ゲームの難易度に対応した要求レベルを満たすプレイヤーに対して通信ゲームの参加を許可する。これにより、初級者が上級者とともに通信ゲームに参加することで上級者の力を借りてゲームを進行するという上記の不都合を解消することができる。

## 【0018】

また本発明では通信ネットワークに接続して通信ゲームを行うときにはゲームの進行状況をセーブデータとして保存しない。また、ゲーム装置がゲーム進行の状況を保存する場合であっても、通信ネットワークに接続しないでゲームを行うときには該進行状況を参照してゲームの途中からプレイすることを禁じるように構成してもよい。これにより、上記の不都合を解消することができる。

## 【0019】

また本発明では通信ネットワークに接続して通信ゲームを行うときにはゲームのエンディング画面の表示時間を短くする。これにより通信ネットワークの接続

料やゲームサーバへのインターネット接続料の増額を抑えることができる。

【 0 0 2 0 】

【発明の実施の形態】

発明の実施の形態 1.

図 1 は記録媒体の第三者による不正使用を防止するサーバとゲーム装置の説明図である。同図において、符号 1 0 は C D - R O M 等のゲームソフトウェアを記録した可搬性記録媒体であり、符号 1 1 は家庭用ゲーム装置である。ゲーム装置 1 1 は記録媒体 1 0 に記録されているゲームプログラムを読み取り、電話回線、I S D N 網等の各種公衆回線或いは専用線等の通信ネットワークを介して他のゲーム装置と共に通信ゲームを行うことができるように所望の通信機能を備えて構成されている。サーバ 1 3 は通信ネットワークに接続する各々のゲーム装置の通信ゲーム処理等を管理する。

【 0 0 2 1 】

記録媒体 1 0 にはシリアルナンバー ( S N ) と呼ばれる各記録媒体に固有の識別情報が与えられている。同図の例では記録媒体の S N は A 0 1 0 1 である。S N は記録媒体 1 0 にデータとして記録されているものでもよく、記録媒体 1 0 或いはその収納ケースやマニュアルに記載されているものでもよい。ゲーム装置 1 1 が通信ネットワークを介してサーバ 1 3 にアクセスすると ( 同図 ( 1 ) ) 、サーバ 1 3 はゲーム装置 1 1 にゲーム装置 1 1 の装置 I D と記録媒体 1 0 の S N の転送を要求する。装置 I D とは各ゲーム装置に対して重複しないように割り与えられた識別情報であり、サーバ 1 3 から発行される。

【 0 0 2 2 】

ゲーム装置 1 1 が初めてサーバ 1 3 にアクセスした場合には、サーバ 1 3 はゲーム装置 1 1 に装置 I D を未だ発行していないため、ゲーム装置 1 1 に装置 I D を発行する ( 同図 ( 2 ) ) 。装置 I D として、ゲーム装置 1 1 がサーバにアクセスした時期を利用することができる。時期には日時である西暦、月、日、時、分、秒が含まれる。例えば、アクセスのあった日時が 2 0 0 0 年 1 2 月 1 0 日 2 1 時 5 分 3 7 秒であった場合には、装置 I D は、2 0 0 0 . 1 2 . 1 0 . 2 1 . 0 5 . 3 7 となる。ゲーム装置 1 1 はサーバ 1 3 から発行された装置 I D をフラッ

シュメモリ等の不揮発性メモリ12に記憶する。また、この日時を暗号化したデータを装置IDとして不揮発性メモリ12に記憶してもよい。

【0023】

データベース14には装置IDをキーとしてゲーム装置に使用された記録媒体のSNが関連付けられてレコード単位で管理されている。サーバ13はゲーム装置11に発行した装置ID(2000.12.10.21.05.37)とSN(A0101)を関連付けたレコードを生成する(同図(3))。

【0024】

上記の構成により、サーバ13はゲーム装置11の装置IDと記録媒体10のSNを関連付けて一元的に管理しているため、第三者が他のゲーム装置で使用された記録媒体を自己のゲーム装置に挿入して使用しようとする、該記録媒体のSNとゲーム装置の装置IDが一致しないため、サーバ13は該第三者の記録媒体の使用に制限をかけることができる。

【0025】

また、2人以上のプレイヤーが秒単位まで含めて同時にサーバにアクセスすることが殆ど皆無であることを考慮すると、装置IDとしてゲーム装置11がサーバ13にアクセスした日時を秒単位まで利用することで、実質的に各ゲーム装置に固有の装置IDを割り当てることができる。勿論、装置IDとして、ゲーム装置がサーバにアクセスした日時のみならず予め重複しないように用意したIDを利用することもできる。

【0026】

尚、上記の説明では記録媒体としてCD-ROMを例示したが、これに限らず、DVD-ROM、DVD-RAM、DVD-R、PDディスク、MDディスク、MOディスク等の各種光ディスク、フレキシブルディスク(FD)、ゲームプログラムを記憶した脱着式カートリッジ、メモリカード等にも適用できる。

【0027】

発明の実施の形態2.

図3はゲーム装置と操作用コントローラの説明図である。操作用コントローラ20にはセーブデータを待避保存するためのバックアップメモリ22を脱着自在

に構成され、さらにアナログキーや各種スイッチを配置した操作部 21 が設けられている。バックアップメモリ 22 は不揮発性メモリを備えている。操作用コントローラ 20 は接続コード 28、及びコネクタ 29 を介してゲーム装置 23 に接続している。尚、バックアップメモリ 22 はゲーム装置 23 に直接脱着自在に取り付けるように構成してもよい。

#### 【0028】

図 2 はゲーム装置と操作用コントローラの機能ブロック図である。ゲーム装置 23 はゲーム処理部 24、暗号処理部 25、CD-ROM ドライブ 26、装置 ID メモリ 27 を備えて構成されている。これらの各モジュールは CPU、ROM、RAM 等のハードウェアによって実現される。ゲーム処理部 24 には CD-ROM ドライブ 26 を介して CD-ROM から供給されるゲームプログラムを読み取り、操作部 21 から出力されるアナログキーや各種スイッチの制御信号を基にゲームを展開し、バックアップメモリ 22 に待避保存するためのセーブデータを生成する。

#### 【0029】

プレイヤーがセーブデータをバックアップメモリ 22 に待避保存するようにゲーム装置 23 に指示を与えるか、若しくはゲームプログラムがプログラム処理の過程でセーブデータを待避保存するようにゲーム装置 23 に指示を与えると、暗号処理部 25 は装置 ID メモリ 27 に記憶されているゲーム装置 23 の固有情報（例えば、製造番号）をキーとしてセーブデータに暗号処理を施し、バックアップメモリ 22 に待避保存する。暗号処理は公知の暗号処理を利用することができる。一方、バックアップメモリ 22 に記憶されているセーブデータをゲーム装置 23 が読み取る場合には、セーブデータは暗号処理部 25 にて装置 ID をキーとして復号処理され、ゲーム処理部 24 に出力される。

#### 【0030】

上記の構成により、バックアップメモリ 22 にセーブされるデータはゲーム装置 23 の固有情報をキーとして暗号化処理されるため、他のゲーム装置で利用することができない。従って、他人のバックアップメモリを利用して自己のゲーム装置でゲームプレイする等のバックアップメモリの不正使用を有効に防止するこ

とができる。

【 0 0 3 1 】

発明の実施の形態 3.

図 4 は複数のゲーム装置が通信ネットワークに接続してゲームプレイを行うときの説明図である。同図において、符号 3 2、3 4 は家庭用ゲーム装置であり、3 5 は通信ゲームの制御を行うサーバである。符号 3 6 は公衆回線等の通信ネットワークである。ゲーム装置 3 2 にはセーブデータを待避保存するためのバックアップメモリ 3 1 0 を備えた操作用コントローラ 3 1 が接続されている。同様に、ゲーム装置 3 4 にもバックアップメモリ 3 3 0 を備えた操作用コントローラ 3 3 が接続されている。通信ネットワーク 3 6 における通信プロトコルはオープンネットワークに適した TCP / IP を用いる。

【 0 0 3 2 】

ゲーム装置 3 2 はゲームの進行に伴い、プレイヤーが獲得したアイテムや、得点、ゲーム進行状況等を適宜、RAM 3 2 0 に書き込む。RAM 3 2 0 に書き込まれたデータはセーブデータとしてバックアップメモリ 3 1 0 に転送可能である。また、プレイヤーが獲得したアイテム等は通信ネットワーク 3 6 を介してゲーム装置 3 4 の RAM 3 4 0 に転送することができる。

【 0 0 3 3 】

図 5 はバックアップメモリに待避保存されたセーブデータを利用して通信ゲームを行うときのバックメモリの状態を示す説明図である。バックアップメモリ 3 1 0 にはアイテム等のセーブデータが待避保存されている。ゲーム装置 2 3 がネットワークに接続すると、バックアップメモリ 3 1 0 内のセーブデータはゲーム装置 2 3 の RAM 3 2 0 に転送（移動）され、バックアップメモリ 3 1 0 内のセーブデータは消去される。このため、ゲーム装置 2 3 が通信ネットワーク 3 6 に接続している間はバックアップメモリ 3 1 0 内のセーブデータは空の状態になっている。ゲーム終了時、RAM 3 2 0 内のセーブデータをバックアップメモリ 3 1 0 に待避保存する際には、RAM 3 2 0 からバックアップメモリ 3 1 0 へセーブデータが転送される。

【 0 0 3 4 】

従来ではバックアップメモリ 3 1 0 のセーブデータを R A M 3 2 0 に転送する場合には、セーブデータをコピーして転送していたため、R A M 3 2 0 にセーブデータを転送した後においてもバックアップメモリ 3 1 0 内にもセーブデータが待避保存されたままの状態であった。このため、プレイヤーがセーブデータの中のパラメータの一部又は全てを他のプレイヤーに提供した場合であっても、その後にバックアップメモリ 3 1 0 を操作用コントローラ 3 1 から強制的に抜き取ることにより、他人に提供したセーブデータを自己のバックアップメモリ 3 1 0 に保存することができる。

#### 【 0 0 3 5 】

しかし、本実施形態によれば、バックアップメモリ 3 1 0 内のセーブデータは R A M 3 2 0 にコピーされるのではなく、R A M 3 2 0 に移動されるため、上記のようなバックアップメモリの不正使用を有効に防止することができる。

#### 【 0 0 3 6 】

発明の実施の形態 4 .

図 6 は通信ゲームの制御を行うサーバとゲーム装置の説明図である。同図において、符号 4 1 は家庭用ゲーム装置であり、サーバ 4 4 にアクセスすることで通信ゲームを行うことができる。ゲーム装置 4 1 は操作用コントローラ 4 2 から供給されるプレイヤーの操作信号を基にゲームを展開する。操作用コントローラ 4 2 にはセーブデータを待避保存するためのバックアップメモリ 4 3 を備えて構成されている。バックアップメモリ 4 3 は不揮発性メモリで構成されている。

#### 【 0 0 3 7 】

サーバ 4 4 はデータベース 4 5 を備えており、ゲーム装置 4 1 のネットワークへのアクセス回数とアクセス日時（以下、アクセス情報という。）を装置 I D をキーとしてレコード単位で記録している。装置 I D とはゲーム装置 4 1 に固有の識別情報であり、例えば製造番号や、ゲーム装置 4 1 が初めてネットワークに接続した日時（秒単位まで含む）等である。同図の例ではゲーム装置 4 1 の装置 I D は B 1 0 1 1、アクセス回数は 7 2 回、アクセス日時は 2 0 0 0 年 1 0 月 2 日 1 9 時 1 4 分 3 2 秒、2 0 0 0 年 1 0 月 4 日 2 1 時 2 5 分 1 1 秒、2 0 0 0 年 1 0 月 9 日 1 1 時 7 分 5 2 秒、…、となっている。ゲーム装置 4 1 のアクセス情報



はデータベース45に登録されとともに、バックアップメモリ43にも同様の内容が書き込まれる。

【0038】

同図において、ゲーム装置41が通信ネットワークを介してサーバ44にアクセスすると（同図（1））、サーバ44はゲーム装置41から装置IDとバックアップメモリ43内のアクセス情報を取得する。次いで、データベース45を参照し（同図（2））、装置IDとアクセス情報が整合するか否かをチェックする。複数のゲーム装置が秒単位まで含めて同一の日時にアクセスすることはほぼない事を考慮すると、アクセス情報はバックアップメモリ43に固有のものと考えられる。このため、ゲーム装置のアクセス情報はバックアップメモリ43を他のバックアップメモリと識別するための識別情報として機能する。

【0039】

装置IDとアクセス情報が一致する場合には、サーバ44はアクセス回数を1だけインクリメントし、アクセス日時を追加記録することでレコード内容を更新する。また同時にバックメモリ43のアクセス情報も更新する（同図（3））。一方、装置IDとアクセス情報が一致しない場合には、バックアップメモリ43の不正使用の疑いがあるため、バックアップメモリ43の使用を制限する。

【0040】

装置IDとアクセス情報が一致しない場合として、①セーブデータを他人のバックアップメモリにセーブして使用しようとした場合、②セーブデータの不正コピーの疑いがある場合である。①の場合は、装置IDとアクセス回数、及びアクセス日時が全く一致しないため、ゲーム装置41に使用されていない他のセーブデータを使用しようとしたことがわかる。②の場合は、ゲーム装置41に使用されたセーブデータであるため、アクセス日時が一部一致するが、アクセス回数が異なるため不正コピーの疑いがある場合である。

【0041】

②の場合について、図7を参照して詳細に説明する。同図に示すように、バックアップメモリ43に記録されたセーブデータをバックアップメモリ46に不正コピーしたとする（同図（1））。バックアップメモリ43に記録されているア

クセス回数は72回とすると、バックアップメモリ46に記録されているアクセス回数も72回になる。ここで、プレイヤーがバックアップメモリ43を使用すると、バックアップメモリ43に記録されているアクセス回数は73回に更新される(同図(2))。また、データベース45内のレコードも73回に更新される(同図(3))。ここで、プレイヤーがコントローラ42からバックアップメモリ43を抜き取り、バックアップメモリ46を新たに装着してサーバ44にアクセスすると、バックアップメモリ46のアクセス回数とデータベース45に記録されているアクセス回数が異なるため、不正コピーの疑いがあるとわかる(同図(4))。また、セーブデータを予め別の記録媒体にコピーしておいて、その後ゲームを行い、セーブデータを更新し、再度更新前のセーブデータに戻してゲームを行うような、同じバックアップメモリを使用する場合も同様である。

## 【0042】

以上、説明したように本実施形態によれば、サーバ44はゲーム装置41の装置IDとアクセス情報を一元的に管理しているため、装置IDとアクセス情報を照合することで、バックアップメモリ43の不正使用、及び不正コピーを有効に防止することができる。

## 【0043】

発明の実施の形態5.

図8は複数のゲーム装置を通信ネットワークに接続して通信ゲームを行う場合の説明図である。同図において、符号51～53は通信ネットワーク54に接続するゲーム装置であり、符号55は通信ゲームの制御を行うサーバである。本実施形態においては、図9に示すように、通信ゲームのレベルに応じてゲーム参加可能なレベルを設定している。例えば、ノーマルレベルでは全員の参加が可能であるが、ハードレベルではレベル20以上、ベリ－ハードレベルではレベル40以上がゲーム参加条件となる。ここでいうレベルとは、ゲームの進行に伴って、プレイヤーキャラクタに与えられるパラメータであり、主に、ゲーム中に倒した敵キャラクタの種類や数に対応して与えられる。

## 【0044】

図8にはハードレベルの通信ゲームを行う場合の各プレイヤーのレベルが記述さ

れており、ゲーム装置51のプレイヤーのレベルは25、ゲーム装置52のプレイヤーのレベルは30、ゲーム装置53のプレイヤーのレベルは45であるから、これら三人のプレイヤーでハードレベルの通信ゲームを行うことができる。

#### 【0045】

従来ではこのような通信ゲームを複数人で行う場合、プレイヤーのレベルを問わずに参加可能であったため、例えば、通信ゲームに習熟したベ上級レベルのプレイヤーと通信ゲームを始めたばかりの初心者が一緒にゲームプレイすることができ、初心者は上級者レベルのプレイヤーの後をついて行くことで、ゲームのエンディングまで辿り着くことが可能となる。このようなレベルの高低を問わずに通信ゲームの自由参加を認めるとゲームの面白さを半減することになりかねない。しかし、本実施形態によれば、通信ゲームのレベルに応じて参加可能なプレイヤーのレベルが設定されているため、上記の不都合を解消することができる。

#### 【0046】

発明の実施の形態6.

図10はゲーム展開のシナリオを記述した説明図である。同図に示すように、ゲームはステージ1～ステージ3までの各ステージから構成される。ステージは森林地帯、地下洞窟、採掘場、古代宇宙船等の場面からなる。各ステージにはゲームの進行に合わせてシーン1、シーン2が設定されており、場面展開に変化を与えている。各ステージにはラスト場面があり、ここに登場する敵キャラクタを倒すことで次ステージに移行することができる。

#### 【0047】

プレイヤーが通信ネットワークに接続せずにオフラインでゲームプレイする場合には、次回のゲームプレイに備えてゲームの進行状況をフラグデータとしてセーブ（保存）しておくのが一般的である。しかし、通信ネットワークに接続してオンラインでゲームプレイする場合には、複数のプレイヤーキャラクタがゲームを展開するため、例えば、初心者は何もしなくても上級レベルのプレイヤーの後をつけていくだけでゲームを進行することができる。

#### 【0048】

このため、本実施形態では図11に示すように、オンラインでゲームを行う場

合には（ステップ S 1 ; Y E S）、ゲーム進行のフラグデータをセーブせず（ステップ S 2）、オンラインでゲームを行わない場合には（ステップ S 1 ; N O）、ゲーム進行のフラグデータをセーブする（ステップ S 3）。かかる構成により、上記の不都合を解消することができる。また、ゲーム装置がゲーム進行のフラグデータを保存する場合であっても、通信ネットワークに接続しないでゲームを行うときには該フラグデータを参照してゲームの途中からプレイすることを禁じるように構成してもよい。

## 【 0 0 4 9 】

尚、通信ゲームの場合にゲーム進行のフラグデータのセーブを制御する手段として、ゲーム装置側にセーブ制御手段を設けてもよく、ゲームサーバの制御によりゲーム進行のフラグデータのセーブを制御するように構成してもよい。

## 【 0 0 5 0 】

発明の実施の形態 7.

図 1 2 にゲームのエンディング画面の画面遷移を示す。同図において、（A 1）～（A 3）はプレイヤが通信ネットワークに接続せずにオフラインでゲームプレイをし、ゲームを終了したときのエンディング画面の画面遷移図である。プレイヤキャラクター 6 1 が敵キャラクター 6 2 を倒し、ゲームが終了すると（同図（A 1））、エンディングスタッフロールが数分間流れ（同図（A 2））、終了画面が表示される（同図（A 3））。

## 【 0 0 5 1 】

一方、（B 1）～（B 2）は複数人が通信ネットワークに接続してオンラインでゲームプレイをし、ゲームを終了したときのエンディング画面の画面遷移図である。プレイヤキャラクター 7 1 ～ 7 4 が敵キャラクター 7 5 を倒してゲームが終了すると（同図（B 1））、速やかに終了画面が表示され（同図（B 2））、元のゲーム画面に戻る（同図（B 1））。

## 【 0 0 5 2 】

このように、プレイヤがオンラインで通信ゲームを行う場合には、回線に接続している限り、電話回線の接続料として電話料金が課金される他、サーバへのインターネット接続料金が課金されるため、ゲームのエンディング画面を短時間で

終了することで、プレイヤの経済的負担を軽減することができる。

【0053】

尚、通信ゲームの場合にゲームのエンディング画面の表示時間を短く制御する手段として、ゲーム装置側に該制御手段を設けてもよく、ゲームサーバの制御によりエンディング画面の表示時間を短く制御するように構成してもよい。

【0054】

【発明の効果】

本発明のセキュリティシステム、記録媒体管理方法及び該方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、通信ネットワークを介してサーバからデータ処理装置に識別情報が発行されるため、データ処理装置に予め識別情報が与えられていない場合でも、どの記録媒体がどのデータ処理装置に使用されたかを管理することができる。

【0055】

本発明のデータ処理装置、データ処理方法及び該方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、バックアップメモリのセーブデータをデータ処理装置に固有の識別情報をキーにして暗号化処理及び復号化処理をすることができるため、セーブデータのセキュリティ対策に効果的である。

【0056】

本発明のデータ処理装置及びセーブデータの管理方法によれば、データ処理装置にてデータ処理されるセーブデータをデータ処理装置に転送した後で、バックアップメモリ内の不揮発性メモリに記憶されたセーブデータを消去するため、セーブデータの不正使用を効果的に防止することができる。

【0057】

本発明のセキュリティシステム、セーブデータの管理方法及び該方法をコンピュータシステムに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、バックアップメモリを備えたデータ処理装置が通信ネットワークに接続した回数をサーバが管理しているため、バックアップメモリ内のセーブデータの不正使用を効果的に防止することができる。

【 0 0 5 8 】

本発明のゲームサーバによれば、ゲームの難易度に対応して通信ゲームに参加可能なレベルを予め設定し、ゲームの難易度に対応した要求レベルを満たすプレイヤーに対して通信ゲームの参加を許可するため、通信ゲームをより面白くすることができる。

【 0 0 5 9 】

本発明のゲーム処理方法及び該方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、通信ネットワークに接続して通信ゲームを行うときにはゲームの進行状況をセーブデータとして保存しないため、通信ゲームをより面白くすることができる。

【 0 0 6 0 】

本発明のゲーム処理方法及び該方法をゲーム装置に実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体によれば、通信ネットワークに接続して通信ゲームを行うときにはゲームのエンディング画面の表示時間を短くするため、通信ネットワークの接続料の負担を軽減することができる。

【図面の簡単な説明】

【図 1】

記録媒体のセキュリティシステムの説明図である。

【図 2】

ゲーム装置とコントローラの説明図である。

【図 3】

ゲーム装置とコントローラの外観説明図である。

【図 4】

ゲーム装置と通信ネットワークの接続構成を示す説明図である。

【図 5】

セーブデータの移動を示す説明図である。

【図 6】

バックアップメモリのセキュリティシステムの説明図である。

【図 7】

バックアップメモリの不正コピー対策の説明図である。

【図 8】

通信ゲームの説明図である。

【図 9】

通信ゲーム参加可能レベルの説明図である。

【図 10】

ゲーム展開のシナリオの説明図である。

【図 11】

ゲーム進行のフラグデータのセーブに関するフローチャートである。

【図 12】

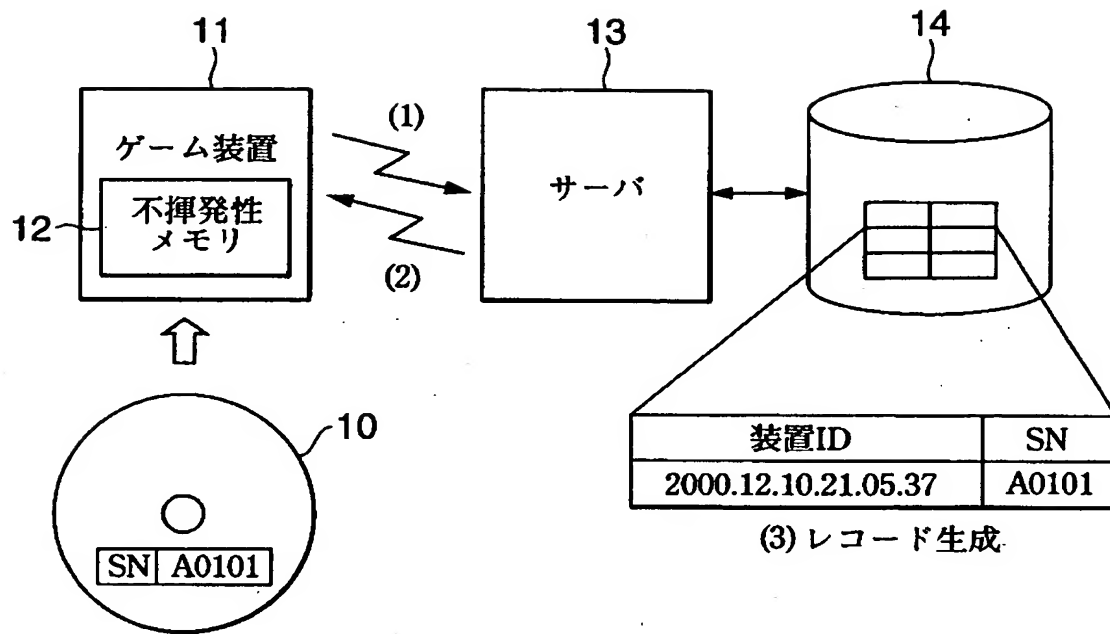
ゲームのエンディング画面の説明図である。

【符号の説明】

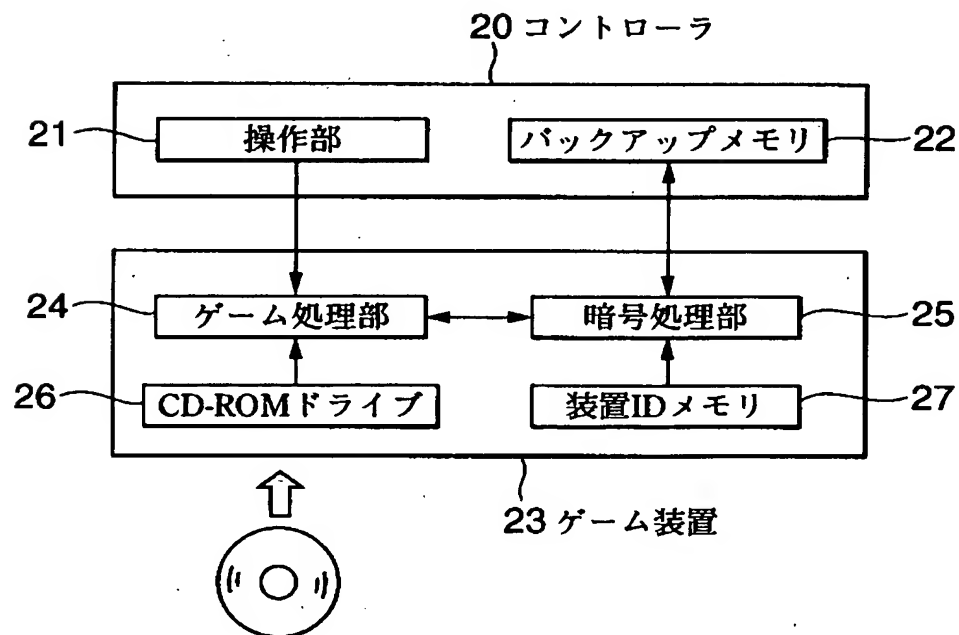
10…CD-ROM、11…ゲーム装置、12…不揮発性メモリ、13…サーバ、14…データベース、20…コントローラ、21…操作部、22…バックアップメモリ、23…ゲーム装置、24…ゲーム処理部、25…暗号処理部、26…CD-ROMドライブ、27…装置IDメモリ、28…接続コード、29…コネクタ、31…コントローラ、32…ゲーム装置、33…コントローラ、34…ゲーム装置、35…サーバ、36…通信ネットワーク、310…バックアップメモリ、320…RAM、330…バックアップメモリ、340…RAM、41…ゲーム装置、42…コントローラ、43…バックアップメモリ、44…サーバ、45…データベース、46…バックアップメモリ、51～53…ゲーム装置、54…通信ネットワーク、55…サーバ

【書類名】 図面

【図 1】

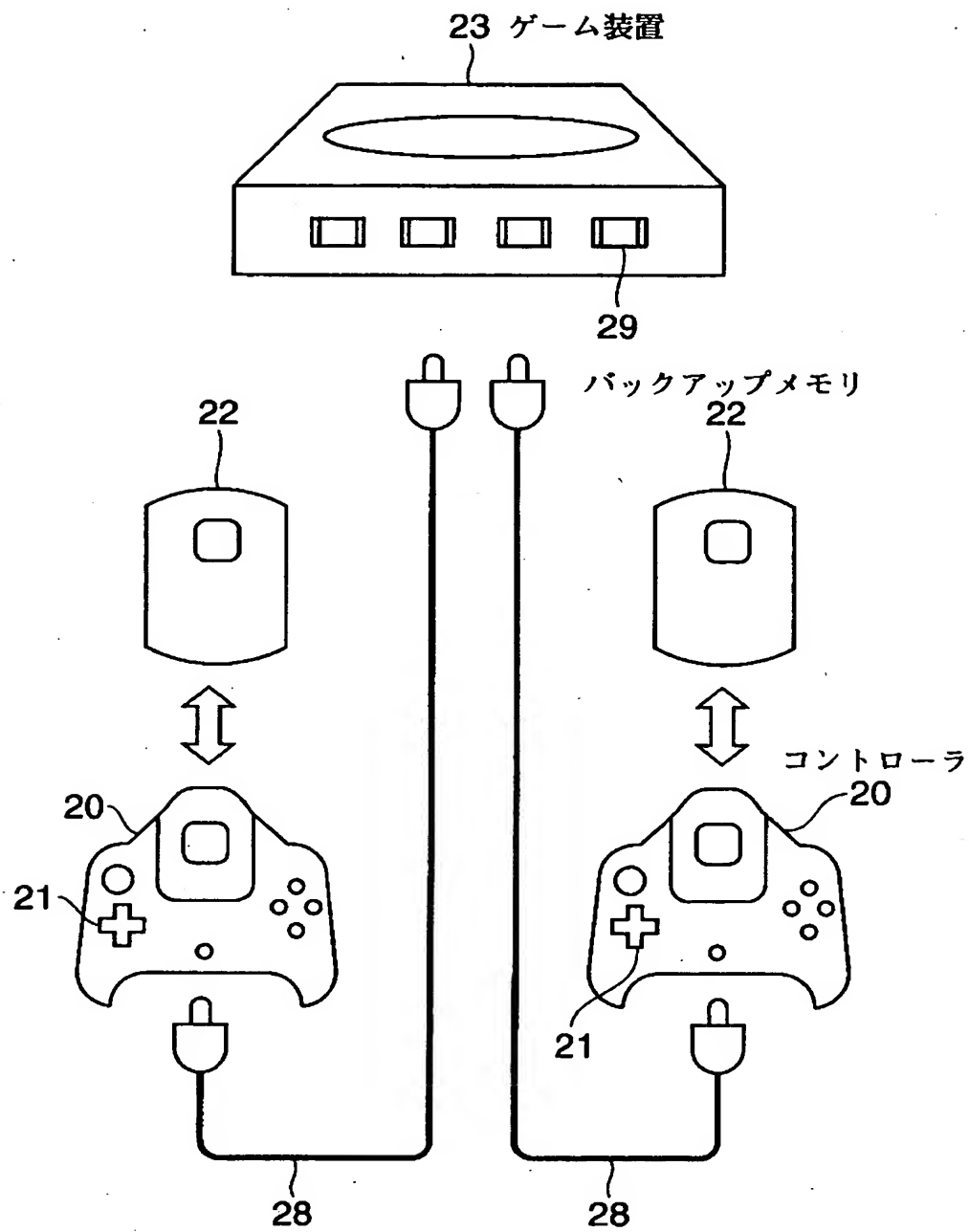


【図 2】

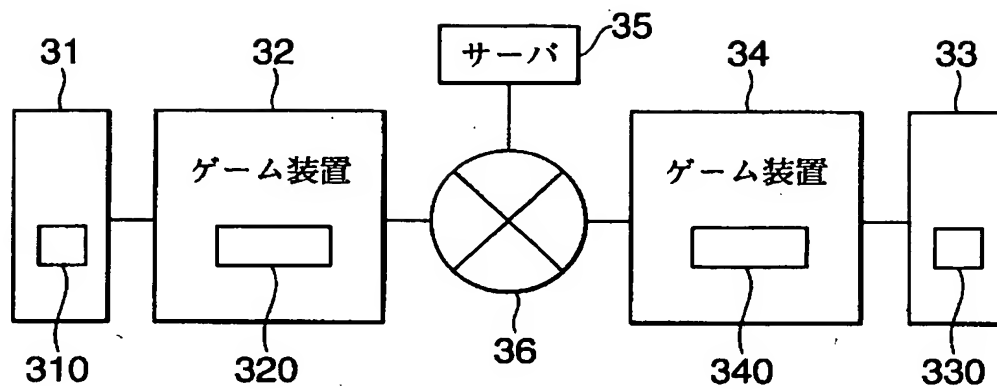




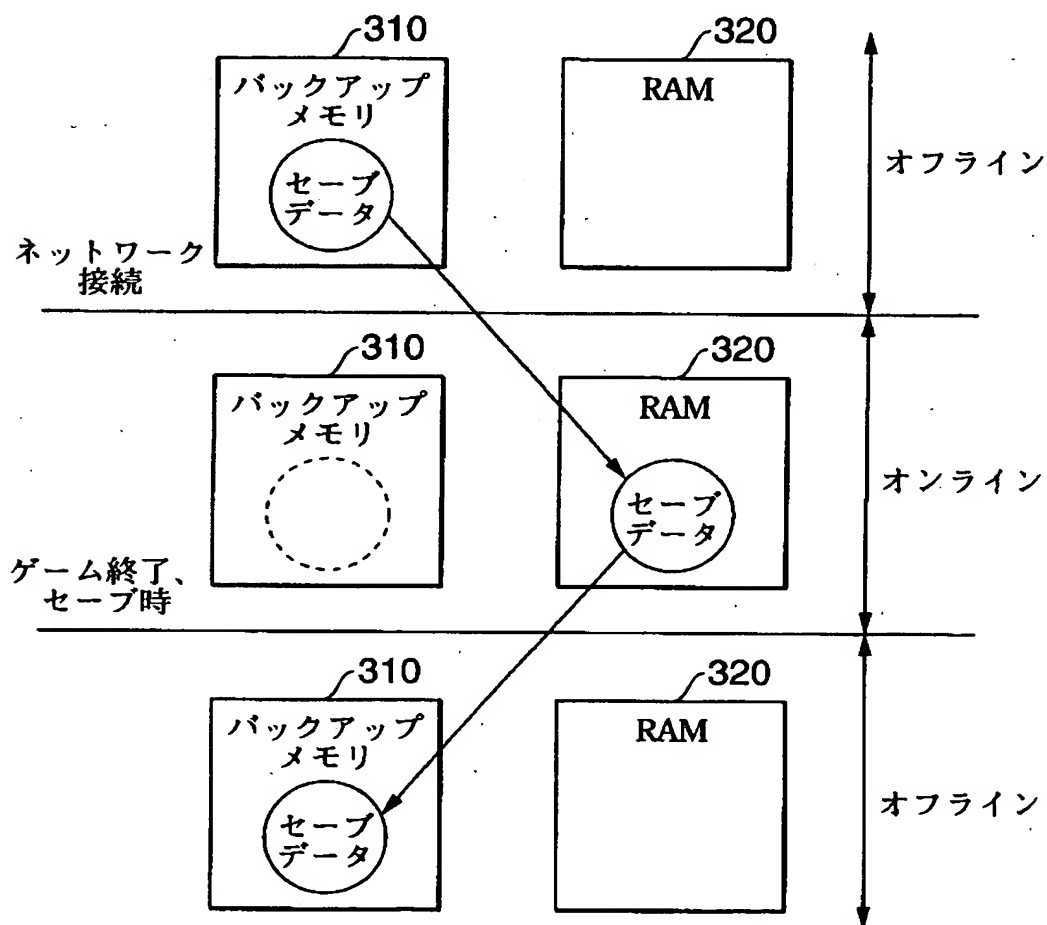
【図3】



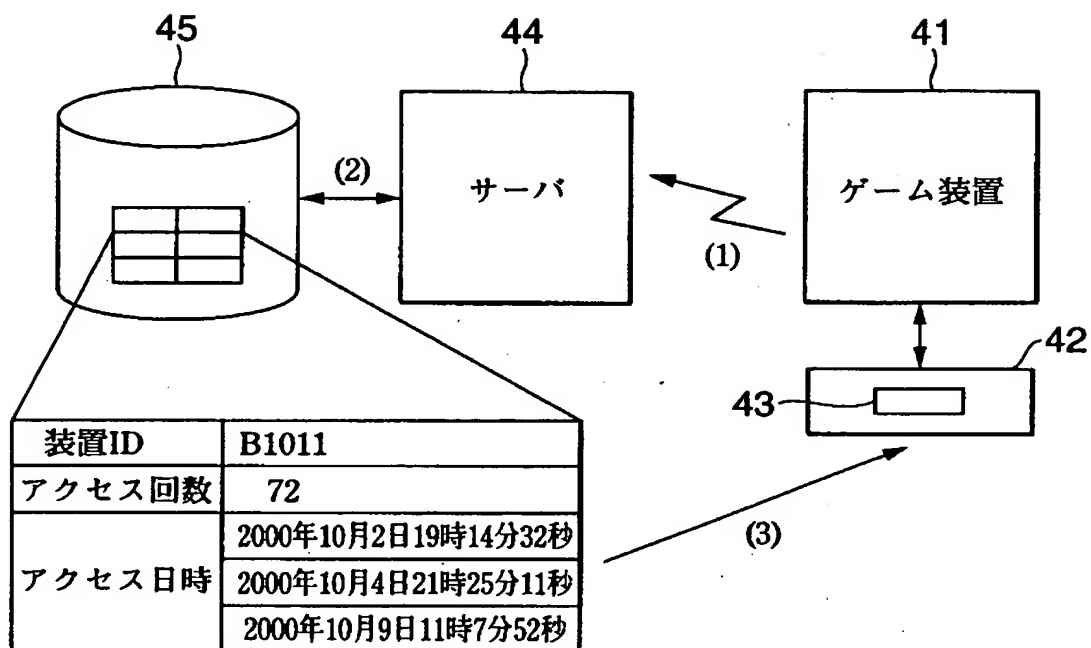
【図4】



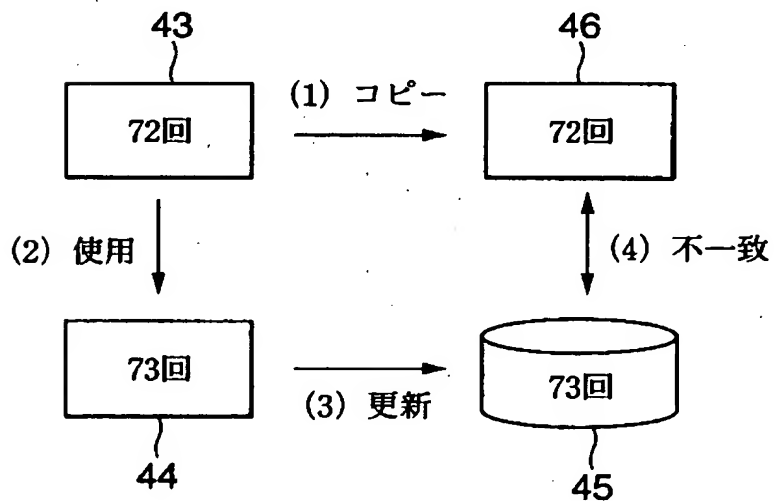
【図5】



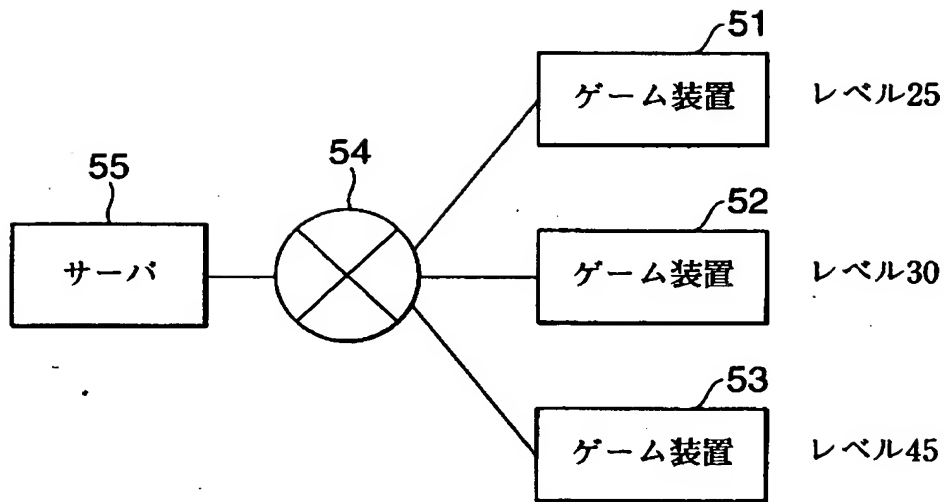
【図 6】



【図 7】



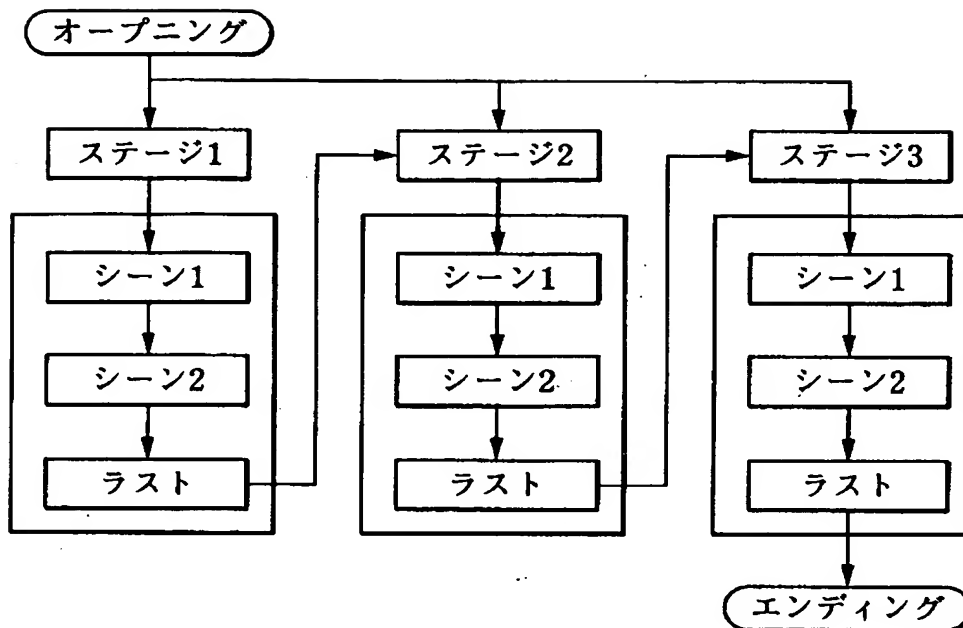
【図 8】



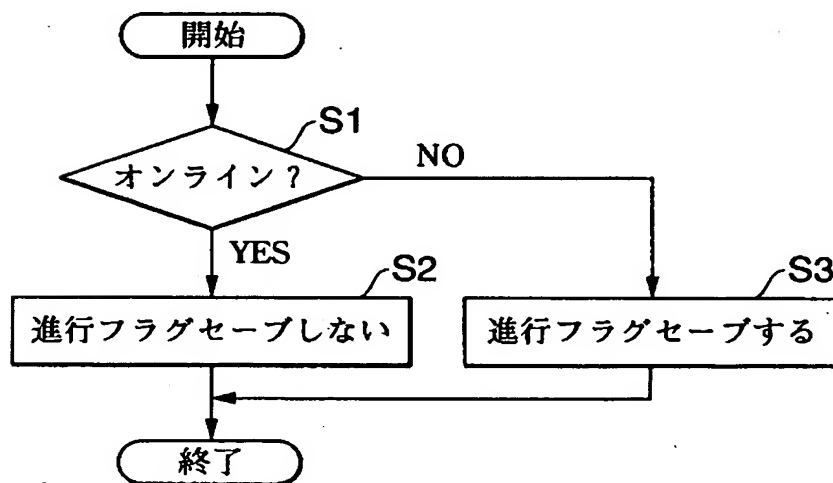
【図 9】

モード	必要レベル
ノーマル	全員可
ハード	20以上
ベリハード	40以上

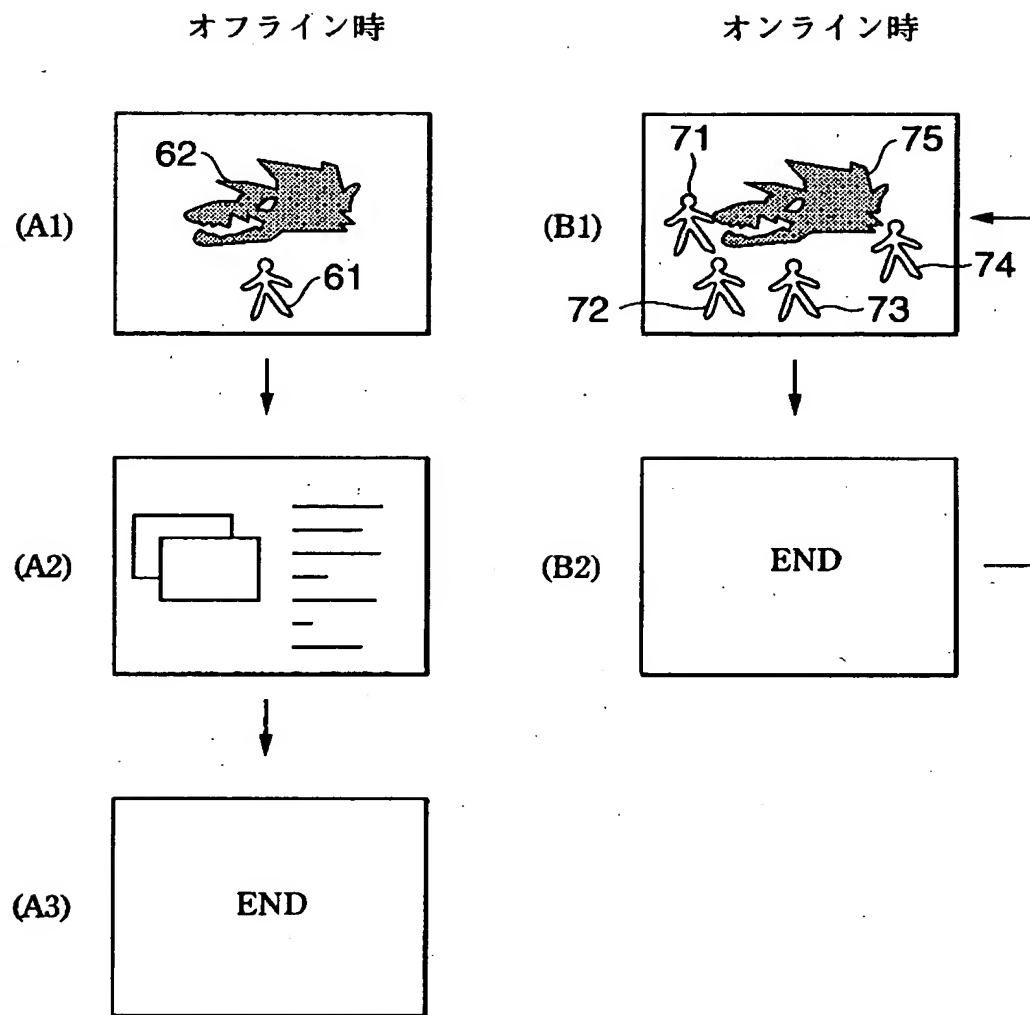
【図10】



【図11】



【図12】



【書類名】 要約書

【要約】

【課題】 予め識別情報をもたないゲーム装置に使用されるCD-ROMがどのゲーム装置に使用されたかを管理するセキュリティシステムを提供する。

【解決手段】 ゲーム装置(11)は通信ネットワークを介してサーバ(13)にアクセスすると、サーバ(13)から発行される装置IDを不揮発性メモリ(12)に記憶する。この装置IDはゲーム装置(11)が通信ネットワークを介してサーバ(13)にアクセスした日時(例えば、2000年12月10日21時5分37秒)を基に生成される。サーバ(13)はゲーム装置(11)に使用されたCD-ROM(10)のシリアルナンバー(SN)とゲーム装置(10)の装置IDを関連付けてデータベース(14)上に登録する。これにより、どのCD-ROM(10)がどのゲーム装置(11)で使用されたかを管理することができる。

【選択図】 図1

認定・付加情報

特許出願の番号	特願2000-387833
受付番号	50001646698
書類名	特許願
担当官	第三担当上席 0092
作成日	平成12年12月21日

<認定情報・付加情報>

【提出日】 平成12年12月20日



出 願 人 履 歴 情 報

識別番号 [000132471]

1. 変更年月日	2000年11月 1日
[変更理由]	名称変更
住 所	東京都大田区羽田1丁目2番12号
氏 名	株式会社セガ